FedRAMP Review and Approve

Standard Operating Procedure

Version 1.2

August 27, 2015

Revision History

Date	Version	Page(s)	Description	Author
08/07/2015	1.0	All	Initial Release	FedRAMP PMO
08/20/2015	1.1	All	Readability corrections; corrected Table 2 on p. 24	FedRAMP PMO
08/27/2015	1.2	All	Remove all links to version-specific documents and replace with non-version-specific links to the website pages where the documents are found.	FedRAMP PMO

How to Contact Us

For questions about FedRAMP or this document, email to info@fedramp.gov.

For more information about FedRAMP, visit the website at http://www.fedramp.gov.

Table of Contents

List of Figures

List of Tables

EXECUTIVE SUMMARY

This document describes the Review and Approve (R&A) process for Authorization Packages for the Federal Risk and Authorization Management Program (FedRAMP) from the first contact by an Applicant (Cloud Service Provider [CSP] or Agency) through posting of the Authorization Package in the FedRAMP Secure Repository. This document serves as a framework for development and integration of a series of subsidiary Standard Operating Procedures (SOP).

As the FedRAMP program is maturing from an (IOC) into a mid-size operating program, this process is designed to be efficient, structured, and scalable. Emphasis is placed on providing sufficient information and online training so that Applicants are prepared to succeed before they apply to FedRAMP. Applicants that respond fully and thoroughly to feedback from the FedRAMP reviewers will move through the FedRAMP R&A process most quickly.

This document supports the ability of FedRAMP to meet its mission and goals of providing a Secure Repository of Authorization Packages available for government use.

1. INTRODUCTION

1.1. PURPOSE

This Standard Operating Procedure (SOP) describes the FedRAMP Review and Approve (R&A) process, which details all of the steps from the first contact by a Cloud Service Provider (CSP) or Agency through the posting of an Authorization Package to the FedRAMP Secure Repository. The R&A process has four phases:

- Phase 1: Prepare and Apply
- Phase 2: Accept for Review
- Phase 3: Perform Initial and Detailed Reviews
  Phase 4: Approve

This process has also been documented in Microsoft Visio: FedRAMP Review and Approve Process Flow Diagram. Excerpts from this diagram are included in this process description. The entire process diagram is available at the following FedRAMP website page: https://www.fedramp.gov/resources/standard-operating-procedures-sops/.

1.2. SCOPE

This process includes activities of the FedRAMP Operations Team, the Quality Management Team, and the FedRAMP Security Team. This SOP provides a high-level description of all of the steps included in FedRAMP's review and approval of a CSP's or Agency's application. In some cases, additional SOPs and associated documents and tools further elaborate specific steps of this R&A process. For example, a separate SOP is available that documents the steps for Security Repository Provisioning (Step. 1.8).

1.3. ROLES AND RESPONSIBILITIES

Role	Responsibilities
Applicant	▪ Takes online training ▪ Prepares Authorization Package ▪ Engages a Third-Party Assessment Organization (3PAO) if necessary
Agency	▪ Submits an application to FedRAMP on behalf of a CSP ▪ Provides documents for an Agency Authorization to Operate (ATO) Authorization Package
FedRAMP Director	▪ Approves completed Authorization Packages
JAB (Joint Authorization Board)	▪ Reviews and approves JAB documents and Authorization Packages
Program Operations Team (Ops Team)	▪ Provides overall program management services to the FedRAMP program
Ops Team Manager	▪ Manages the Ops Team ▪ Is a government employee

Role	Responsibilities
Communications Specialist	▪ Provides communication vehicles (for example, guides, website) ▪ Guides Applicant through online documentation and training ▪ Answers questions from Applicants
Training Specialist	▪ Develops on-line training
Secure Repository Administrator The FedRAMP Secure Repository is managed by the Office of Management and Budget (OMB). The Secure Repository is referred to as MAX.	▪ Provides access to the FedRAMP Secure Repository for Applicants ▪ Directs Applicant where to upload documents ▪ Validates that packages/documents have been upload correctly in MAX
Lead Reviewer	▪ Schedules and conducts CSP interview ▪ Queues reviews ▪ Initiates and oversees the Level 1 review ▪ Updates Salesforce as needed to reflect status changes ▪ Sends Level 1 Review Results to Applicant
Quality Management (QM) Technician	▪ Performs Level 1 Completeness, Showstopper, and Readability Reviews ▪ Submits their completed checklists and reviews to the Lead Reviewer
Security Team	▪ Performs the Detailed Review of Application Packages, and is also responsible for Continuous Monitoring
Information Systems Security Officer (ISSO)	▪ Receives reviewed Authorization Packages from Lead Reviewer ▪ Holds kickoff meeting with Applicant ▪ Conducts Detailed Review ▪ Prepares Authorization Packages for JAB Provisional Authorization to Operate (P-ATO)

1.4. MANAGEMENT COMMITMENT

Management commitment to this procedure is based on a chain of authorizing documents originating with the OMB FedRAMP Memorandum of December 8, 2011, which authorizes the establishment of FedRAMP. Following that, the *Guide to Understanding FedRAMP* describes FedRAMP's responsibility for reviewing and approving Authorization Packages. See the Introduction and FedRAMP Review and Approval Process Overview sections of the *Guide* for more detailed information on review and approval. The *Guide* can be downloaded from the following FedRAMP website page: https://www.fedramp.gov/resources/documents/.

1.5. COORDINATION AMONG ORGANIZATIONAL ENTITIES

The FedRAMP program is evolving from an Initial Operating Capability (IOC) into a more mature program and has, in tandem, experienced a significant growth in team size. As with any organization that experiences rapid growth, there is a risk of poor communications and missed handoffs among organizational entities unless explicit steps are taken to promote the smooth flow of information among FedRAMP Program Management Office (PMO) teams. The

development of a single commonly understood process linking all team activities is an important step to ensure FedRAMP continues to effectively execute as it grows.

Development of a commonly accepted and repeatable R&A Process is an also important step towards process improvement, a key goal of the FedRAMP Program.

FedRAMP PMO Operations is responsible for managing the FedRAMP Initial Review process (hereafter referred to as the Initial Review). FedRAMP PMO Quality Management supports the Initial Review process and reports their results to Operations. Operations in turn notifies the Ops Team leader, the Applicant, and the Security Team of the Initial Review results. A description of the Initial Review is available at the following FedRAMP website page: https://www.fedramp.gov/resources/standard-operating-procedures-sops/.

CSPs, 3PAOs, JAB members, and Federal Agencies may request access to the FedRAMP Secure Repository. The FedRAMP Secure Repository Administrator approves or denies access to the FedRAMP Secure Repository, and provisions the approved requests. No additional coordination is required between the entities granted Secure Repository access.

1.6. COMPLIANCE

Overall, the R&A process supports the FedRAMP Program goals to comply with relevant Federal I/T security standards. As the *Guide to Understanding FedRAMP* states:

> *FedRAMP processes are designed to assist Agencies in meeting FISMA requirements for cloud systems and addresses complexities of cloud systems that create unique challenges for complying with FISMA.*[1]

In addition, compliance can have different meanings during different phases of the R&A Process:

- Phase 1: Prepare and Apply:
  - Applicants satisfy all application and training requirements at the beginning of the R&A process.
- Phase 2: Accept for Review
  - Applicants use correct FedRAMP templates and file naming conventions when submitting documents or packages for review.
  - Applicants, JAB members and staff, 3PAOs, and FedRAMP staff only use the FedRAMP Secure Repository on MAX for exchange and storage of sensitive security documents.
  - The Secure Repository Administrator ensures that the Applicant has completed all required training before approving access to MAX.
- Phase 3: Perform Initial and Detailed Reviews
  - The Ops Team (that is, the Lead Reviewer and the QM Technician) and the Security Team follow defined checklists during the Initial Review and FedRAMP Detailed Reviews (hereafter referred to as the Detailed Review).

[1] See the Guide to Understanding FedRAMP (p.9) at the following FedRAMP website page: https://www.fedramp.gov/resources/documents/.

  - In order to pass Initial Review, an Authorization Package or document must be complete, free from Showstoppers, not lacking key critical controls, and readable.
  - In order to pass Detailed Review, a package or document must pass a rigorous, checklist-driven security review by a FedRAMP ISSO. A description of the Detailed Review is available at the following FedRAMP website page: https://www.fedramp.gov/resources/standard-operating-procedures-sops/.
- Phase 4: Approval
  - The JAB and FedRAMP Director follow the Federal Information Security Management Act (FISMA) and FedRAMP requirements when deciding to approve an Applicant document or Authorization Package.
  - A CSP has satisfactorily completed a FedRAMP assessment and is granted an ATO when the cloud system meets the following requirements:
    - The system authorization package has been created using the required FedRAMP templates.
    - The system meets the FedRAMP security control requirements.
    - The system has been assessed by an independent assessor (3PAO or Agency designated assessors).
    - At least one of the following three:
      1. A Provisional Authorization from the JAB. Cloud systems with a FedRAMP P-ATO path have undergone a rigorous technical review by the FedRAMP PMO, been assessed by a FedRAMP accredited 3PAO, and received a P-ATO from the Department of Homeland Security (DHS), the Department of Defense (DOD), and General Services Administration (GSA) Chief Information Officers (CIOs).
      2. A CSP with an Agency ATO that meets the above FedRAMP package requirements. Cloud systems listed under the Agency Authorization have worked directly with a customer Agency to achieve a FedRAMP compliant ATO that has been verified by the FedRAMP PMO.
      3. A CSP Supplied complete package that has passed the Initial Review for all system documentation (System Security Plan [SSP], Security Assessment Plan [SAP], Security Assessment Report [SAR], and supporting documents). Cloud systems listed under the CSP Supplied Package path have submitted to the FedRAMP PMO a completed Security Package that has been assessed by a FedRAMP accredited 3PAO.
    - An authorization letter for the system is on file with the FedRAMP PMO (with the exception of CSP supplied packages).
    - The CSP maintains the continuous monitoring requirements of FedRAMP. Failure to meet continuous monitoring, introduction of significant changes, or increase in risk posture may invalidate the package and result in removal of FedRAMP compliance.

1.7. PREREQUISITES

The overall R&A process is initiated by a contact from an Applicant (a CSP or Agency) to FedRAMP indicating an interest to pursue a FedRAMP review. FedRAMP requires Applicants

to take FedRAMP's online training before granting access to FedRAMP's Secure Repository. The Applicant must also complete an application in order to initiate the R&A process.

Applicants must use FedRAMP's contact and inquiry email address (info@FedRAMP.gov) to initiate contact with the FedRAMP team. Applicants must use FedRAMP's Secure Repository (MAX) to upload Authorization Packages and documents to FedRAMP. The FedRAMP Website (www.FedRAMP.gov) is an important information resource for Applicants. Salesforce and the GSA Google Drive are required for internal use by the FedRAMP team. Additional tools may be used in the future.

Applicants, before submitting their Authorization Package for review, should ensure that it meets all FedRAMP requirements.

2. FEDRAMP REVIEW AND APPROVE PROCESS OVERVIEW

2.1. INTRODUCTION TO REVIEW AND APPROVE PROCESS

Figure 1 is an end-to-end diagram of the FedRAMP R&A Process. It comprises four stages, each of which is described in the sections below. The figure shows the main activities of the CSP/Agency Applicants and FedRAMP staff, as well as inputs to data repositories such as MAX (for secure storage), Blackboard (for training), and Salesforce (for tracking). Due to the size of the diagram, the graphic below is meant to be illustrative. A full size PDF of this diagram is available at the following FedRAMP website page: https://www.fedramp.gov/resources/standard-operating-procedures-sops/.

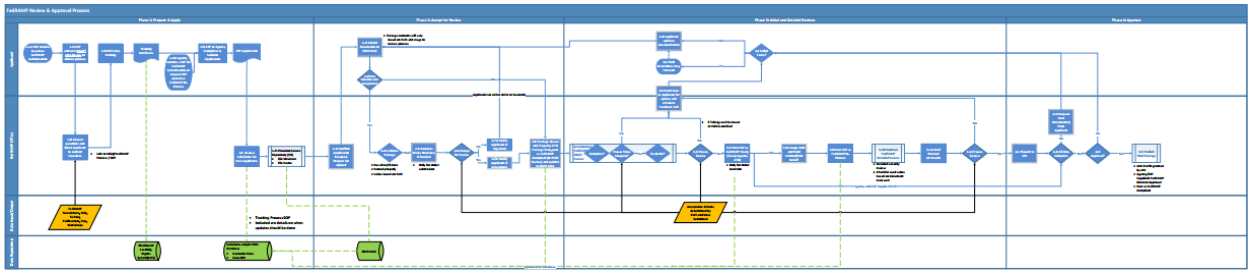

Figure 1: FedRAMP Review and Approve Process

There are two major entry points to the process:

1. A CSP submits an application for its cloud service product for review and approval.
2. An Agency submits a CSP product for FedRAMP review and approval.

There are three possible end-points of the process:

1. Posting of an Authorization Package on the FedRAMP website as "FedRAMP Compliant"[2] and posting into the FedRAMP Secure Repository.
2. Decision by an Agency or CSP to put their application on hold in order to develop a more complete Authorization Package.
3. Rejection of the Agency or CSP Authorization Package due to significant shortcomings in the Authorization Package despite repeated rounds of feedback and guidance from the FedRAMP team.

2.2. AUTHORIZATION PACKAGE CATEGORIES/PATHS

As described in the *Guide to Understanding FedRAMP*, there are three paths for security packages to make their way into the FedRAMP Secure Repository:

- JAB P-ATO Path: CSP Authorization Packages are reviewed by an accredited 3PAO and then reviewed by both FedRAMP ISSOs and the JAB and result in a P-ATO.

[2] For a definition of FedRAMP Compliant, see the Guide to Understanding FedRAMP (p.12) at the following FedRAMP website page: https://www.fedramp.gov/resources/documents/.

- CSP Supplied Path: CSPs may submit an Authorization Package to FedRAMP for prospective Agency use. In this case, a CSP pursues the FedRAMP process independently instead of through an Agency or the JAB. If successful, at the end of this process, a CSP's package can be deemed FedRAMP compliant but no ATO or P-ATO is issued.
- Agency ATO Path: Agencies can submit an Authorization Package on behalf of a CSP. Typically, an Agency uses a 3PAO to conduct an assessment. If the Authorization Package is assessed as FedRAMP compliant, the Agency can also submit the package to the JAB and seek a P-ATO.

The list of required documents is the same for all three paths, except that the Agency ATO path includes an Agency ATO Letter. Appendix B: Required Authorization Package Documents lists the required documents for a complete Authorization Package. In general, for Agency and CSP Supplied, a complete Authorization Package must be submitted and is reviewed in aggregate from the start.

For the JAB P-ATO path, the process is more iterative. The *initial* submission to FedRAMP consists only of the SSP and applicable attachments. Once the SSP is approved by the JAB, the Applicant must submit the SAP, which will go through a review similar to the one performed for the SSP (with different checklists; for example, 2.4 Validate Package, 3.1 Initial Review), followed by review of SAR, which will also undergo a similar set of checks.

2.3. FedRAMP Ready, FedRAMP In-Process, and FedRAMP Compliant (In PMO Review)

While being assessed by FedRAMP, Authorization Packages can be designated as FedRAMP Ready or FedRAMP In-Process.

FedRAMP Ready is a milestone step in becoming FedRAMP Compliant, but it is not a final determination. FedRAMP Ready is a designation for Applicants that are in the CSP Supplied path, JAB P-ATO path, or have not decided between the CSP Supplied, Agency ATO, or JAB P-ATO paths. To be listed as FedRAMP Ready, Applicants must pass an Initial Review of their SSP and all SSP attachments (see Appendix B: Required Authorization Package Documents).

Once an Applicant has been listed as FedRAMP Ready, they have one year to decide a path (if undecided), submit the remaining package documentation, and pass the Initial Review. If the completed authorization package does not pass an Initial Review within a year, the Applicant will no longer be designated as FedRAMP Ready.

FedRAMP Ready CSPs have proven they are ready for FedRAMP PMO Detailed Review required to become FedRAMP Compliant and gives agencies the confidence that the SSP documentation meets the FedRAMP PMO's quality and security standards that are necessary to initiate the assessment and authorization process with the JAB.

FedRAMP In-Process is a designation for Applicants that are in the JAB P-ATO or Agency ATO paths. The purpose of FedRAMP In-Process is to signify:

- Either, a CSP is working actively with an Agency on a FedRAMP Authorization and has committed to meeting the FedRAMP security requirements through that Agency.

- Or, a CSP has completed the Initial Review and has been assigned a FedRAMP ISSO to work through meeting the FedRAMP security requirements through the JAB. Additionally, the CSP will have engaged the services of an accredited 3PAO to complete its security assessment.

In addition, an Agency reviewing an Authorization Package (with or without FedRAMP's involvement) can request the Authorization Package be listed as In-Process on the FedRAMP website.

FedRAMP Compliant (In PMO Review) is a designation for Agency ATO Authorization Packages only. This designation signifies that the CSP's cloud system has been granted an ATO by an Agency and has submitted all required documentation for review to the FedRAMP PMO. Once the FedRAMP PMO completes the Initial Review of the package, the CSP will be listed as FedRAMP Compliant.

Table 1 summarizes how packages are assigned FedRAMP In-Process and FedRAMP Ready designations based on path.

Table 1. FedRAMP Designations by Path

Path	FedRAMP In-Process Designation	FedRAMP Ready Designation	FedRAMP Compliant (In PMO Review)
JAB P-ATO	A CSP passes the FedRAMP Initial Review, an ISSO is assigned, and a kickoff meeting is held.	A CSP passes the FedRAMP Initial Review (SSP and all attachments).	N/A
Agency ATO	A CSP is actively working with an Agency on a FedRAMP Authorization but does not have an Agency ATO yet, or has sent the FedRAMP PMO a complete package.	N/A	A complete package is delivered to the PMO and has an Agency ATO but hasn't completed an Initial Review.
CSP Supplied	N/A	A CSP's cloud system passes the FedRAMP Initial Review (SSP and all attachments).	N/A

3. PHASE 1: PREPARE AND APPLY

Figure 2 illustrates how a CSP or Agency prepares and applies to FedRAMP.

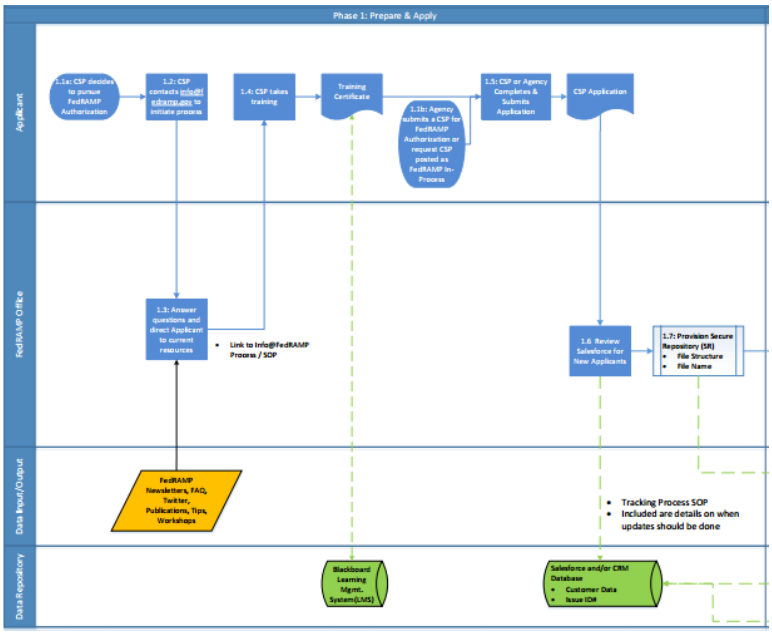

Figure 2: Phase 1: Prepare and Apply

Each CSP is responsible for gathering necessary information and preparing for the FedRAMP review. It must document how it meets the security requirements, and may need to engage an independent 3PAO to test its security implementation.

Step 1.1a: The CSP Decides to Pursue FedRAMP Authorization

The R&A process begins when a CSP decides to pursue a FedRAMP Authorization. The CSP may research resources available on www.fedramp.gov. It may also contact the general FedRAMP mailbox info@fedramp.gov with questions. Whenever possible, the Communications Specialist or other FedRAMP staff person directs the CSP to existing information vehicles and instructs the CSP to take the required online training course. In some cases, the Communications Specialist may research unusual or highly technical questions and provide individualized answers. A CSP can pursue a CSP Supplied Agency ATO or the JAB P-ATO path.

Step 1.1b: An Agency Submits a CSP for FedRAMP Authorization

The FedRAMP process can also begin when an Agency submits an Authorization Package for review. In this case, the Agency has used a FedRAMP accredited 3PAO or Agency specific independent trusted third-party assessment organization to assess its package and is now ready to submit the package to FedRAMP for review. In addition, an Agency can request that FedRAMP post a CSP product as FedRAMP Ready at any time if the Agency is currently assessing a CSP regardless of whether or not an Authorization Package for that CSP product has been submitted to FedRAMP.

Step 1.2: CSP Contacts info@FedRAMP.gov to Initiate the Process

During this initial stage, the CSP will send an email to info@fedramp.gov and communicate its intention to submit an application to have its cloud services evaluated for FedRAMP compliance. This is true regardless of the path followed. The Communication Specialist monitors the info@fedramp.gov account and notifies the Operations Team Manager of the new CSP's intention to participate in the FedRAMP program.

Step 1.3: Answers Questions and Directs Applicant to Current Resources

During the application process, the Applicant can send questions to the info@fedramp.gov email account. A FedRAMP Communication Specialist will respond to its questions, typically within one working day of submission. The Communication Specialist will also direct the CSP to information on the program on the FedRAMP website.

The FedRAMP website provides detailed information on program requirements, the application and document submission process, and the review process. Information is also available through various communication vehicles including online documents, FAQs, Newsletters, Weekly Tips, Workshops, and Twitter posts. FedRAMP also provides online training that explains the process and the related documents. These resources and activities are handled by the Communication Specialist and the Training Specialist, supported by other members of the FedRAMP Team as needed**.**

Step 1.4: CSP Takes Training

Whether it contacts FedRAMP or not, the CSP starts by taking specific required modules of the FedRAMP Online Training, available through the website and hosted on Blackboard Learning Management System (LMS). Training modules contains online tests of the material content. All CSPs must take the training, regardless of the intended path. Currently, all Applicants take the same course; however, additional courses are planned.

Step 1.5: CSP or Agency Completes and Submits Application

With the training certificate and the self-assessment completed, the CSP may apply to FedRAMP. The CSP fill outs and submits the application at www.fedramp.gov and attaches the required pre-application forms. An Agency could also fill out the application. The application requests basic information about the Applicant, such as company name and contact information. In some cases, the FedRAMP PMO may provide assistance filling out the application. An application must be filled out by a CSP or Agency, regardless of the path followed.

Step 1.6: Review Salesforce for New Applicants

The application submission automatically triggers creation of a unique ID in Salesforce (a Customer Relationship Management [CRM] tool) and generates an email acknowledgement to the Applicant (CSP or Agency) and to FedRAMP, which includes the unique ID. The Secure Repository Administrator manually reviews Salesforce and then triggers a request for provision in MAX. An Applicant Tracking Process SOP, detailing process tracking and notification, is planned.

Step 1.7: Provision Secure Repository

After receiving the acknowledgement, the Secure Repository Administrator begins to provision the CSP access to MAX. The MAX Secure Repository SOP provides details on this process. Appendix B lists the specific files that must be uploaded to MAX for a CSP, Agency, or JAB P-ATO path package.

4. PHASE 2: ACCEPT FOR REVIEW

Figure 3 illustrates how FedRAMP collects CSP information and documentation.

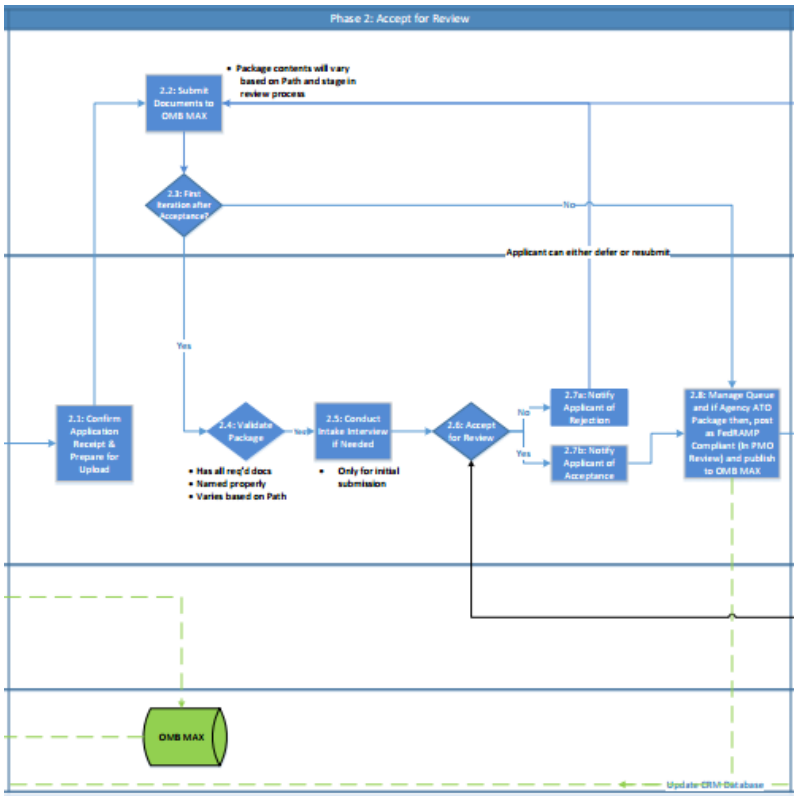

Figure 3: Phase 2: Accept for Review

The Applicant is responsible for providing all required package documentation with the proper file naming conventions. The Secure Repository Administrator notifies the Applicant of the location in MAX for document upload and validates that all documents are uploaded successfully. The Lead Reviewer follows up with the Applicant to validate the received information and proposed path, and to discuss the review process. The Lead Reviewer then notifies the QM Reviewer that the package has been accepted for review. This process is the same regardless of path.

Step 2.1: Confirm Application Receipt and Prepare for Upload

Once the Secure Repository Administrator has granted MAX access to the Applicant, the Secure Repository Administrator contacts the Applicant to confirm receipt of the application and provide the naming convention and location for the Applicant to upload required documents. The list of documents to upload is largely the same, with some variation depending on the authorization path (see Appendix B: Required Authorization Package Documents). This step is executed for all paths.

Step 2.2: Submit Documents to MAX

Based on guidance from the Secure Repository Administrator, the Applicant uploads its documents to MAX. Note that this step could occur multiple times, depending on where an Applicant is in the review process. For example, if a document or package is rejected in Initial Review, then the Applicant is expected to correct the documents and resubmit them to MAX. This step is executed for all paths.

Step 2.3: First Iteration after Acceptance

In addition, once an application is accepted, the package will be validated (see Step 2.4) and an Intake Interview (see Step 2.5) held between the Applicant and the Lead Reviewer. However, if a package fails a later quality check such as an Initial Review, a second Intake Interview is not required. Similarly, another package validation is not required unless asked for by the Lead Reviewer or ISSO.

Step 2.4: Validate Package

Once an Applicant uploads its package, the Secure Repository Administrator checks that all required documents are included, properly named, and do not require passwords. If any required documents are missing, misnamed, or cannot be opened, the Secure Repository Administrator notifies the Applicant that it needs to submit additional, renamed, or unencrypted documents. Once all required documents are present, are properly named, and can be opened, the Secure Repository Administrator notifies the Lead Reviewer by email that the package is ready for initial review, and updates the CSP system status in Salesforce. The Secure Repository Administrator notifies the Applicant by email that the package has been validated—that is, contains all of the required files correctly named. This step is executed for all paths.

Step 2.5: Conduct Intake Interview

The Lead Reviewer reviews the submitted materials and schedules and conducts a phone interview with the Applicant to confirm that it may proceed with the FedRAMP Authorization process, and to answer any questions from the Applicant. The proposed path is also reviewed. This step is executed for all paths.

Step 2.6: Accept for Review

The Lead Reviewer determines if the Applicant is ready to proceed based on the package submitted, the proposed path, and the results of the Intake Interview. The Lead Reviewer notifies the Applicant of the decision by email. This step is executed for all paths.

Step 2.7a: Notify Applicant of Rejection

If package is not accepted for review, the Lead Reviewer contacts the Applicant by email and asks the Applicant to revise its documentation and resubmit. If there are special sensitivities regarding the package or the submitter (especially an Agency), the Lead Reviewer will consult with the FedRAMP Director or Ops Manager. This step is executed for all paths.

Step 2.7a: Notify Applicant of Acceptance

If the Lead Reviewer determines that the package is complete and ready to move on to the next phase, the Lead Reviewer places the Applicant's package in the queue of packages awaiting

review, notifies the Applicant by email, and provides an estimated date for completion (including a margin of additional time for unexpected circumstances). This queue is owned and managed by the Lead Reviewer and maintained using Google Docs. This step is executed for all paths. Note: The estimated date will vary by path and will evolve based on the implementation of the new Initial Review process and report, potential automation, and the team's experience.

Step 2.8: Manage Queue and if Agency ATO Package, then post as FedRAMP Compliant (In PMO Review) and Publish to MAX

The Lead Reviewer notifies the Ops Manager by email that the package is ready for review and has been added to the queue of packages to be reviewed based on predefined acceptance criteria. When the Lead Reviewer receives an Agency ATO Package the Lead Reviewer will also notify the Communications Specialist to post the system as FedRAMP Compliant (In PMO Review) and the Secure Repository Administrator to publish the Authorization Package to MAX. The management of the queue is executed for all paths.

5. PHASE 3: PERFORM INITIAL AND DETAILED REVIEWS

Figure 4 illustrates the Initial and Detailed Reviews of all packages. All packages, regardless of path, go through the Initial Review. JAB packages also go through a FedRAMP Detailed Review performed by an ISSO.

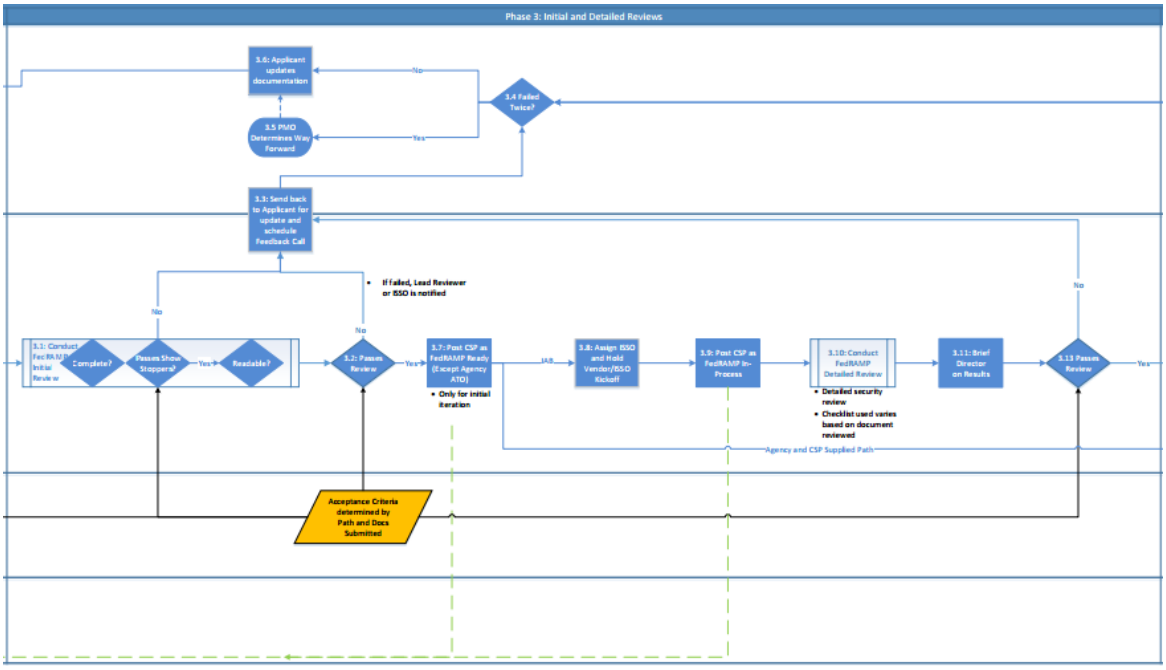

Figure 4: Phase 3: Perform Initial and Detailed Reviews

The Initial Review is made using Quality Assurance (QA) documentation standards plus additional checks on key technical areas, with defined criteria for acceptance.

JAB P-ATO: If the package passes the Initial Review criteria, an ISSO on the FedRAMP Security team performs a more detailed technical review. If the package fails the Initial Review criteria, the Authorization Package is returned to the Applicant to be updated (see Step 3.3).

Agency or CSP Supplied: If Authorization Package passes the Initial Review criteria, it goes to Step 4.2, which validates that all documents have been completed in the package and it is ready for review by the FedRAMP Director. If a package fails the Initial Review criteria, the Lead Reviewer documents the results of the Initial Review using the Initial Review Results report template and sends the results to the Applicant.

Step 3.1: Conduct Initial Review.

The Initial Review has three parts: (1) a Completeness review (2) a "Showstoppers" review, and (3) a Readability review. A package must pass all parts in order to continue to the next step. For a JAB P-ATO path package, the next step is a Detailed Review conducted by an ISSO from the Security Team. For the CSP Supplied or Agency ATO path package, the next step is validating that the documents have been submitted prior to a review by the FedRAMP Director.

The three parts of the Initial Review are described in more detail below.

3.1a Completeness: The Completeness Review is the same for all paths and uses the same document checklist templates. However, the documents that are submitted may vary (see Appendix B: Required Authorization Package Documents).

The Quality Control (QC) Technician checks that the documents use the required FedRAMP templates. For documents without mandatory templates, the QC Technician checks that they are in Microsoft Office formats and that the required information is provided. If the package is an Agency ATO, the QC Technician next checks the Agency ATO Letter for required elements, and examines the system's risk posture based on the Table of Open Risks from the SAR against FedRAMP-established thresholds. The specific items to be reviewed are contained in the Initial Review SOP Checklists and will vary based on the path followed (that is, Agency, CSP Supplied, or JAB) and the document being reviewed (for example, SSP or SAR).

3.1b Showstoppers: Regardless of whether or not a package has passed the Completeness test above, the QC Technician executes a high-level security review of the package. In this step, the QC Technician reviews a package for "Showstoppers," which are missing, incomplete, or weak critical security controls that must be addressed before the document can be submitted for further FedRAMP review. The Initial Review SOP Checklist contains the list of Showstoppers and critical controls to be checked.

If the package fails either the Completeness or Showstoppers test, the QC Technician notifies the Lead Reviewer, identifying the problems. The Lead Reviewer sends an email to the Applicant informing them of the results of the Initial Review, including problems identified (Step 3.3).

3.1c Readability:

If the package passes both the Completeness and Showstoppers tests, the package must pass a Readability test, which means that it must be consistent, concise, and clear. The QC Technician will use the FedRAMP Readability Review Template to perform a readability review of the documents. If the QC Technician reports to the Lead Reviewer that an Authorization Package has a readability problem, the Lead Review may require the Applicant to correct the Authorization Package.

Step 3.2: Passes Initial Review

When a JAB P-ATO path document passes Initial Review, the Lead Reviewer notifies the Applicant and provides the Initial Review Results, which includes the completed checklists and the QC Technician's comments. The Lead Reviewer also notifies the FedRAMP Director that the Initial Review has been completed and the documents are acceptable under the FedRAMP standards.

If a JAB P-ATO document passes all Initial Review tests, the package or document is passed to the FedRAMP Security Team. The Lead Reviewer notifies the Security Team that the document is ready for the Detailed Review and notifies the CSP that the package has passed Initial Review. If the package does not pass all Initial Review tests, the JAB package is sent back to the Applicant (Step 3.3).

Upon completion of the review for Agency or CSP Supplied packages, the QC Technician notifies the Lead Reviewer. The QC Technician's checklist is supplied as part of the notification.

The Lead Review will notify the Applicant if the package has passed. If the package does not pass, the Agency or CSP Supplied package is sent back to the Applicant (Step 3.3).

In all cases, the Lead Reviewer updates status information in Salesforce.

Step 3.3: Send Back to Applicant

If a package fails the Initial Review, the Lead Reviewer will provide written feedback to the Applicant for all paths using the Initial Review Results Report (L1RR) Template. The L1RR will contain the checklist of Showstoppers and Critical Controls reviewed in Initial Review and commentary noting whether this requirement was met. In addition, the QC Technician and the Lead Reviewer will conduct a telephone call with the Applicant to review the feedback and determine how the Applicant can bring the documentation up to standards. Once the Applicant incorporates the feedback and makes the recommended updates, the Applicant resubmits the documents to the MAX Secure Repository and notifies the Lead Reviewer of the resubmission.

Step 3.4: Failed Twice?

If a document fails either Initial Review or Detailed reviews twice, the PMO will determine the way forward. This check is intended to discourage Applicants from going through multiple rounds of review.

Step 3.5: PMO Determines Way Forward

If a package has failed Initial Review or Detailed Review twice, the FedRAMP Director will determine the way forward. Options include:

- Instituting a waiting period for the Applicant before the Applicant can resubmit the application.
- Allowing the Applicant another chance to submit the package.

Once determined, the Lead Reviewer will inform the Applicant of the waiting period or opportunity for resubmission.

Step 3.6: Applicant Updates Documentation

Based on feedback from the FedRAMP team, the CSP or Agency updates their package or document and resubmits the package to MAX (Step 2.2).

Step 3.7: Post CSP as FedRAMP Ready (Except Agency ATO)

To be listed as FedRAMP Ready on www.fedramp.gov, a package must successfully pass the FedRAMP Initial Review of the SSP and attachments. This Initial Review signifies that the FedRAMP PMO believes that the documentation the CSP provided meets the minimum quality standards to begin the ATO process. Once a CSP has passed the Initial Review, the Lead Reviewer will notify the Applicant and the Communications Specialist will update the website referencing the CSP as FedRAMP Ready.

Note: Once a CSP Supplied package is complete and has passed its FedRAMP Initial Review, the package can be submitted to the FedRAMP Director to be designated FedRAMP Compliant. A CSP Supplied package may be submitted incrementally, similar to a JAB path—that is, submit

SSP first, followed by a SAP/SAR. The minimum requirement to enter an Initial Review is a complete SSP.

Step 3.8: Assign ISSO and Conduct Vendor/ISSO Kickoff (JAB Path)

If a package or document successfully passes Initial Review and the Applicant is seeking an authorization from the JAB, an ISSO is assigned by the Security Team Lead. The ISSO will organize a kickoff meeting, either in person or by phone, to inform the Applicant of the status of their application and the process going forward. A kickoff meeting is only held when the package is going to Detailed Review for the first time.

Step 3.9: Post CSP as FedRAMP In-Process

Once a CSP on the JAB P-ATO path has passed the Initial Review, and has been assigned and met with an ISSO, the Authorization package will be designed In-Process. The Lead Reviewer will notify the CSP Applicant and the Communications Specialist will update the website.

Step 3.10: Conduct FedRAMP Detailed Review

The Detailed Review is a detailed security review conducted by an ISSO. Depending on the document being reviewed, the ISSO reviewer will use a different checklist. Detailed Review checklists are documented in a separate SOP.

Step 3.11: **Brief Director on Results**

Regardless of the results of Detailed Review, the ISSO reviewer will periodically brief results of the reviews to the FedRAMP Director. If the Authorization Package passes the Detailed Review, the FedRAMP Director will make the final decision as to whether a package is ready to be submitted to the JAB.

Step 3.12: Passes Detailed Review?

If the package or document passes Detailed Review and has been approved for submission by the FedRAMP Director to the JAB, it will be presented to the JAB to be considered for a P-ATO. If it fails, a notice about the document or package is sent to the Applicant to be updated (Step 3.4). However, it will typically not require a new Initial Review unless determined by the ISSO.

6. PHASE 4: APPROVE

Figure 5 below illustrates Phase 4, Approve phase.

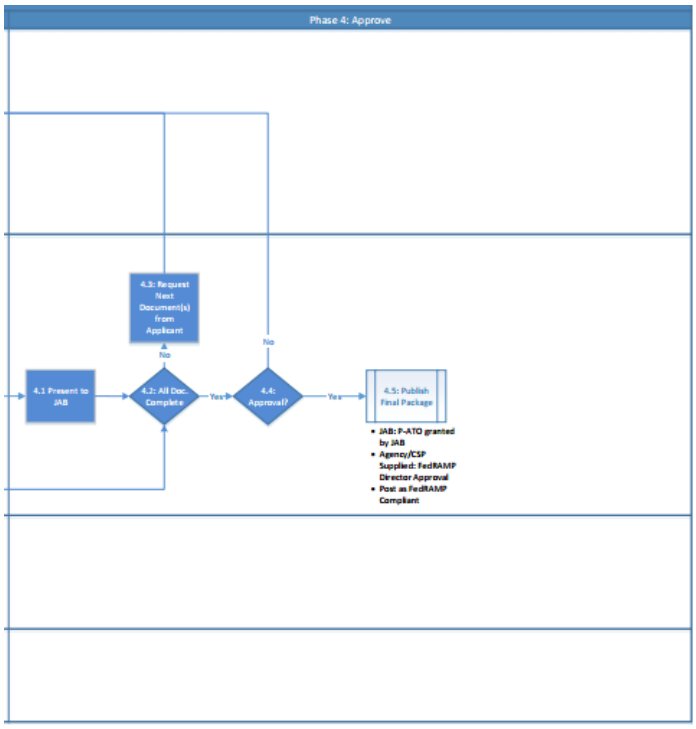

Figure 5: Phase 4: Approve

Step 4.1: Present to JAB:

The results of the Detailed Review will be presented to the JAB. The JAB can either accept or reject the package. If it is rejected, the Applicant is expected to update the package (Step 3.3).

Step 4.2: All Docs Complete?

For packages on the JAB P-ATO path, the SSP must be approved first by the JAB before the SAP or SAR can be completed and submitted. The SAP and SAR will also go through the Initial Review and the Detailed Review, using appropriate checklists based on document type.

For packages on the Agency or CSP Supplied path, the ISSO will determine if additional documents are needed. If so, the ISSO will contact the Applicant (Step 4.3). Otherwise, the package will be submitted to the FedRAMP Director (Step 4.4).

Step 4.3: Request Next Document from the Applicant

If additional documents are required to complete the Authorization Package, the ISSO will contact the Applicant and request the next document(s) to be evaluated. The Applicant will submit the missing documents using Step 3.6, Applicant Updates Documentation.

Step 4.4: Approval?

Once all documentation for the JAB P-ATO path are completed and approved by the JAB, the JAB will grant a P-ATO. For a CSP Supplied package, the CSP is asked to present a SAR briefing to the FedRAMP Director prior to approval for posting. Similarly, a complete Agency supplied package will be presented to the FedRAMP Director for approval.

Step 4.5: Publish Final Package

For Agency ATO and CSP Supplied packages, once the Director has approved, the Lead Reviewer informs the Communications Specialist to announce the Authorization Package status on the Fedramp.gov website as FedRAMP Compliant and notifies the Point of Contact (POC) from the authorizing Agency and the CSP that the package has been listed. All of the steps needed for completing this step are in the Publish Final Package SOP.

7. REFERENCED FEDRAMP DOCUMENTS

Title	Description
Applicant Tracking Process SOP	Process for how an Applicant's progress through the R&A process will be tracked and reported
Continuous Monitoring SOP	Process for performing the continuous monitoring of technical packages that have been granted a P-ATO by JAB
CSP Supplied/Agency Initial Review Results Report Template	Template for the report sent to the CSP or Agency for the CSP Supplied or Agency ATO path detailing the results of the Initial Review
Info@FedRAMP SOP	Process for responding to questions and issues submitted via info@fedramp.com
Initial Review Checklists	The checklists used in the Initial Review, which will vary by path
Initial Review SOP	Process for executing the first set of reviews overseen by the Lead Reviewer, which include checks for Completeness, Showstoppers & Critical Controls, and Readability (clear, concise, consistent)
Detailed Checklists	The checklists used in Detailed Review, only used for JAB packages
Detailed Review SOP	Process for executing the detailed ISSO-led review of a JAB package
MAX Secure Repository SOP	Process for managing the MAX repository
Publish Final Package SOP	Process for updating the FedRAMP Secure Repository and website once a package is reviewed and approved for ATO or P-ATO
Training & Initiation Process SOP	Process for creating training and initiation material for the FedRAMP program

APPENDIX A: TABLE OF ACRONYMS

Acronym	Meaning
3PAO	Third-Party Assessment Organization
ATO	Authorization To Operate
CIS	Control Implementation Summary
CM	Configuration Management
CRM	Customer Relationship Management
CSP	Cloud Service Provider
FedRAMP	Federal Risk and Authorization Management Program
FIPS	Federal Information Processing Standard
FISMA	Federal Information Security Management Act (of 2002)
GSA	General Services Administration
JAB	Joint Authorization Board
IOC	Initial Operating Capability
IR	Incident Response
ISSO	Information Systems Security Officers
IT	Information Technology
LMS	Learning Management System
N/A	Not Applicable
OMB	Office of Management and Budget
P-ATO	Provisional Authorization to Operate
PDF	Portable Document Format
PIA	Privacy Impact Analysis
PMO	Program Management Office
POA&M	Plan of Action and Milestones
POC	Point of Contact
PTA	Privacy Threshold Analysis
QA	Quality Assurance
QM	Quality Management
ROB	Rules of Behavior

Acronym	Meaning
SAP	Security Assessment Plan
SAR	Security Assessment Report
SOP	Standard Operating Procedure
SSP	System Security Plan

APPENDIX B: REQUIRED AUTHORIZATION PACKAGE DOCUMENTS

The following documents are required regardless of path, except for the Agency ATO Letter, which is only required for the Agency ATO path. When a FedRAMP template is not available, NIST Special Publication 800 Series guidance should be followed. Applicants on the JAB P-ATO path will submit the SSP first, followed by the SAP, SAR, and Plan of Action and Milestones (POA&M) in sequence as the previous documents are completed and approved by the JAB TRs.

Table 2. Required Authorization Package Documents and Attachments

Item No.	Document Title (attachments indented)	FedRAMP Template Available?	Agency Path	CSP Path	JAB Path	Undecided Path
1.0	System Security Plan (SSP)	Yes	✔	✔	✔	✔
1.1	FIPS Pub 199	Yes	✔	✔	✔	✔
1.2	e-Authentication	Yes	✔	✔	✔	✔
1.3	Information System Security Policies & Procedures	No	✔	✔	✔	✔
1.4	Configuration Management Plan (CM) Plan	No	✔	✔	✔	✔
1.5	Control Implementation Summary (CIS)	Yes	✔	✔	✔	✔
1.6	CIS Worksheet	Yes	✔	✔	✔	✔
1.7	IT Contingency Plan (CP) and CP Test	Yes	✔	✔	✔	✔
1.8	Incident Response Plan (IRP)	No	✔	✔	✔	✔
1.9	Privacy Threshold Analysis (PTA) / Privacy Impact Assessment (PIA)	Yes	✔	✔	✔	✔
1.10	User Guide	No	✔	✔	✔	✔
1.11	Rules of Behavior (ROB)	Yes	✔	✔	✔	✔
1.12	Signature Page	No	✔	✔	✔	✔
2.0	Security Assessment Plan (SAP)	Yes				
2.1	Rules of Engagement (ROE)	No	✔	✔	✔	✔
2.2	Security Assessment Test Cases	Yes	✔	✔	✔	✔
3.0	Security Assessment Report (SAR)	Yes				
3.1	Security Assessment Report	Yes	✔	✔	✔	✔
3.2	Security Test Cases	Yes	✔	✔	✔	✔
3.3	Vulnerability Scans	No	✔	✔	✔	✔
3.4	Ad Hoc Evidence	No	✔	✔	✔	✔
4.0	Plan of Action and Milestones (POA&M)	Yes	✔	✔	✔	✔
5.0	Agency ATO Letter (provided as PDF)	Yes	✔			
	[See Notes on Following Page]					

Notes:
✔ = Required for initial package submission
✔ = Must be submitted eventually, but not with initial package submission. For undecided, CSPs have 12 months to select a path and submit missing documents. For JAB, missing documents are submitted based on a schedule developed by the CSP and ISSO. See section 2.2 for a description of the JAB path.